UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,360	05/09/2001	Gopikrishna T. Kumar	10007291-1	4719

22879 7590 05/30/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

NOTIFICATION DATE	DELIVERY MODE
05/30/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/852,360
Filing Date: May 09, 2001
Appellant(s): KUMAR ET AL.

Ashok K. Mannava
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/28/08 appealing from the Office action mailed 8/31/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Kocher et al., "The SSL Protocol Version 3.0", March 1996, Internet Draft, draft-freier-ssl-version3-01.txt, pg. 1-60.

5,931,917	Nguyen	8-1999
6,167,382	Sparks	12-2000

6,643,701	Aziz	11-2003
6,367,009	Davis	4-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 3, 4, 11 – 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Aziz et al. (Aziz), U.S. Patent, 6,643,701.

Regarding claim 1, Aziz discloses:

generating at the gateway module respective first session identifiers upon receipt of initial requests from the mobile communication devices at the gateway module and transmitting the first session identifiers to the application program (8:15-22). Herein, Aziz discloses that requests from a device causes the relay ["gateway module"] to conduct an SSL handshaking session with the server

["application program"]. Thus Aziz discloses the establishment of an SSL connection (Aziz, fig. 2:230, see also fig. 3:330) between two end points (Aziz 8:23, the relay, and the server) and the generation and transmission of session identifiers ["first session identifiers"] which are sent by the relay to the server. This is evidenced by the teachings of Kocher for the SSL protocol (Kocher et al., "The SSL Protocol Version 3.0"). An SSL handshake between two end points begins with the client first creating and sending a 'Client hello' message to the server, the message comprising a session identifier (Kocher, pg. 21, sect. 7.6.1.2, par. 1,2; compare also Aziz 1:59-63 and 8:23 – the "relay" and "server" constitute the end points of an SSL connection, or a "client" and "server").

associating the first session identifiers with corresponding second session identifiers from the application program at the gateway module (8:15-33). Again, Aziz shows the use of the SSL protocol. According to protocol, the application program "processes the client hello message and responds with either a handshake_failure or server hello message" (Kocher, pg. 23, 7.6.1.3 "Server hello"). Thus, the application program (Aziz, fig. 3:340) sends session identifiers within a server hello message ["second session identifiers"] (Kocher, pg. 23, "session_id") to the gateway (Aziz, fig. 3:320). The second session identifiers corresponds in a manner to the first session identifiers, thereby allowing the gateway module to appropriately manage a potential plurality of concurrent SSL communications sessions existing between a plurality of clients and the application server (Aziz, fig. 3).

wherein respective connections are established between the mobile communications devices and the application program (Aziz, fig. 3:[300.1 – 300.M], fig. 3:340).

and in response to subsequent communications from the mobile devices to the application program (Aziz, 7:58-64; 8:25-32),

while the respective connections between the mobile devices to the application program are established (Aziz, fig. 3:[310.1 – 310.M], fig. 3:340) *and for communications within the respective sessions* (Aziz has disclosed that these separate sessions between the devices and application program are for communication, 6:29-44),

transmitting from the gateway module to the application program the second session identifiers that are associated with the first session identifiers of the mobile devices of the subsequent communications (Aziz, 8:25-32; Kocher, pg. 19, par. 1,2; Kocher, pg. 24, sect. 7.6.1, "session_id"). Herein, Aziz discloses that resumed communications (subsequent communications) from a device result in a SSL session, comprising the sending from the gateway module to the application program the same session_id value as was previously sent from and stored in memory by the application program. This session_id value, identifying the session to be resumed, corresponds to the second session identifier sent by the server within the Server hello message during the initial establishment of the session.

Regarding claim 2, Aziz discloses:

receiving requests of a first type from the mobile devices at the gateway module and transferring the first type requests to an authentication module that manages user authentication (8:66 – 9:5);

and when a user at a mobile device has not logged-in to the authentication module, transmitting a log-in prompt from the authentication module to the mobile device in response to a request of the first type from the mobile device (9:3-5,23-29). Herein, Aziz discloses that when the server requires client authentication, the server requests (the client is prompted) that the client transmit log in information.

Regarding claim 3, Aziz discloses:

generating at the authentication module respective authentication identifiers for the first session identifiers and associating the authentication identifiers with corresponding first session identifiers (2:11-15, 31-36; 8:66 – 9:5,23-29). Herein, Aziz discloses that resulting at the authentication module ("generating"), are authentication identifiers associated with the identifiers of the session.

Regarding claim 4, it is the apparatus implementing the method of claim 1, and it is rejected, at least, the same reasons.

Regarding claims 11 – 13, they are system implementing the method of claims 1 – 3, and they are rejected, at least, for the same reasons. Furthermore, Aziz discloses a "mobile interface", an interface to connect with a plurality of mobile devices (fig. 3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of Davis et al. (Davis), U.S. Patent 6,367,009.

Regarding claim 5, it is a method substantially similar to the method of claim 1, and it is rejected, at least, for the same reasons. Furthermore, Aziz discloses applications of client – server technology within e-commerce and banking systems. Thus, Aziz makes clear that sessions between clients and a server are sessions between clients and a "merchant" application (1:40-55). Additionally Aziz, discloses that client devices can be wireless devices such as cell phones (7:4-18). However, Aziz does not explicitly disclose that a wireless device would establish a session with the gateway using wireless means, and therefore, that session identifiers are associated with wireless sessions.

Davis, in a substantially similar disclosure as Aziz, discloses that a wireless device (client) can utilize its wireless functionality to establish wireless sessions (fig. 3; 7:30-39, 8:44-67).

It would have been obvious to one of ordinary skill in the art to employ the teachings of Davis within the system of Aziz. This would have been obvious because one of ordinary skill in the art would have seen logical the use of a wireless device to establish a wireless session. Thus, the combination of Aziz and Davis discloses the use of a wireless device to establish a SSL session wirelessly, and therefore, that the session identifiers would be wireless session identifiers.

Regarding claim 10, it is the apparatus implementing the method of claim 5, and it is rejected, at least, the same reasons.

Claims 6 – 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Aziz and Davis, in view of Sparks et al., "Design and Production of Print Advertising and Commercial Display Materials Over the Internet", U.S. Patent 6,167,382.

Regarding claim 6, the combination of Aziz and Davis does not disclose receiving checkout requests from the wireless communication devices at the gateway module and transferring the

checkout requests to a wallet module that manages user authentication. Instead, the combination of Aziz and Davis discloses a generic system for establishing communications between a client and a server via a gateway (Aziz, figs. 2 and 6). The client and server each establish a secure session connection with an intervening relay. The relay then enables communications between the client and the server. The combination of Aziz and Davis discloses that this system is used as an improvement to various publicly available systems such as electronic commerce and shopping systems where the authentication and encryption of information is necessary (Aziz, col. 1, lines 42-47; col. 3, lines 1,2). However, it was not the purpose of the combination of Aziz and Davis to discuss the methods and features specific to the e-commerce and shopping systems. Thus, the combination of Aziz and Davis does not disclose methods such as receiving checkout requests, transmitting payment options, or using wallet identifiers.

Sparks discloses a system that features the electronic commerce methods of receiving checkout requests, transmitting payment options, and using wallet identifiers (Sparks, col. 2, lines 36-49; col. 17, lines 12-26).

It would have been obvious to one of ordinary skill in the art to combine electronic commerce features, such as those disclosed by Sparks, with the generic system of the combination of Aziz and Davis for establishing communications because it is obvious that a generic system designed to enhance electronic commerce (Aziz, col. 1, lines 42-47) would need to features to enable electronic commerce.

Thus, the combination of Aziz, Davis, and Sparks discloses:

receiving checkout requests from the wireless communication devices at the gateway module and transferring the checkout requests to a wallet module that manages user authentication (Sparks,

col. 2, lines 36-49; Aziz, fig. 2; Sparks, Abstract, lines 6-9; 5:41-43; 16:57-67). Herein, the combination enables for a client device to send checkout requests that are received at the gateway module and transferred to a e-commerce server application which receives the checkout requests and authenticates the buyer [thus, a "wallet module"].

when a user at a wireless communications device has logged-in to the wallet module, transmitting payment options from the wallet module to the wireless communications device in response to a checkout request from the wireless communications device (Sparks, figs. 3, 4, 9, 59, 60);

when a user at a wireless communications device has not logged-in to the wallet module, transmitting a log-in prompt from the wallet module to the wireless communications device in response to a checkout request from the wireless communications device (Sparks, figs. 3, 4).

Regarding claim 7, the combination of Aziz, Davis, and Sparks disclose:

generating at the wallet module respective wallet session identifiers for the wireless session identifiers and associating the wallet session identifiers with corresponding wireless session identifiers in a wallet session identifier table (Sparks, figs. 21 – 23).

Regarding claim 8, the combination of Aziz, Davis, and Sparks disclose:

in response to a payment request from a wireless communications device, transmitting the payment request from the gateway module to the merchant application (Sparks, col. 10, lines 37-64; Aziz, fig. 2);

disassociating the wireless session identifier from the corresponding merchant session identifier (Aziz, col. 2, lines 57-67; col. 6, lines 45-55). Unless session resumption procedures have

been initiated by the client or the server, the session identifiers of the client are not re-associated with the corresponding session identifiers of the server, therefore, they are disassociated.

generating a new wireless session identifier for the wireless communications device when another initial request is received from the wireless communications device (Aziz, col. 6, lines 45-55). New sessions can be requested by the client.

Regarding claim 9, the combination of Aziz, Davis, and Sparks implies *clearing inactive entries from the wallet session identifier table.* Electronic systems are not limitless in means for storage and operation. If unnecessary information was never cleared from memory, eventually such systems would reach their limits of storage. Therefore, it would have been obvious to one of ordinary skill in the art to clear inactive entries from the table in order to free and efficiently use a limited amount of memory.

Claim 1 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen et al. (Nguyen), "System, Method, and Article of Manufacture for a Gateways System Architecture with System Administration Information Accessible from a Browser", U.S. Patent 5,931,917 in view of Davis et al. (Davis), U.S. Patent 6,367,009.

Regarding claim 1, Nguyen discloses:

generating at the gateway module respective first session identifiers upon receipt of initial requests from the communication devices (63:32-34,38-40 – notice initial requests from communication devices) *at the gateway module and transmitting the first session identifiers to the application program* (fig. 20c:2010; 65:28-48 – notice generated first session identifiers uniquely identifying an individual transaction that has been submitted by one of the communication devices);

associating the first session identifiers with corresponding second session identifiers from the application program at the gateway module. Second session identifiers from the application (fig. 20:2005; 61:4; 65:59-63 -TIDs are issued by the bank) are associated with the first session identifiers (fig. 20C:2010, see also 64:36-38) which are generated by the gateway to uniquely represent a corresponding transaction request received from a client.

wherein respective connections are established between the communications devices and the application program (fig. 22).

and in response to each subsequent communication from each device to the application program via the connection between the device and the application program while the connection is established, transmitting from the gateway module to the application program the second session identifier that is associated with the first session identifier of the devices of the subsequent communication (19:4-9; 20:10-22).

Regarding claim 1, the examiner notes that Nguyen does not explicitly state that communication devices may be described as mobile. However, Nguyen makes clear that a user may employ any computing device from any location in the world for the purpose of conducting commercial transactions (63:32-38).

Davis discloses that it was well known in the art for users to employ mobile computing devices to conduct commercial transactions (1:48-66; 8:44-67). It would have been obvious to one of ordinary skill in the art to recognize the teachings of Davis for *mobile* computing devices within the teachings of Nguyen for *any* computing device. This would have been obvious because one of ordinary skill in the art would have been motivated to employ known and useful methods of prior art.

Regarding claim 2, the combination discloses:

receiving requests of a first type from the mobile devices at the gateway module and transferring the first type requests to an authentication module that manages user authentication; and when a user at a mobile device has not logged-in to the authentication module, transmitting a log-in prompt from the authentication module to the mobile device in response to a request of the first type from the mobile device (figs. 28, 29, 31).

Regarding claim 3, the combination discloses:

generating at the authentication module respective authentication identifiers for the first session identifiers and associating the authentication identifiers with corresponding first session identifiers (88:24-44).

Regarding claim 4, it is the apparatus implementing the method of claim 1, and it is rejected, at least, the same reasons.

Regarding claim 5, it is rejected, at least, for the same reasons as claim 1, and furthermore, because the combination discloses the use of wireless communications between system elements (Davis, 1:48-66; 8:44-67).

Regarding claim 6, the combination discloses:

receiving checkout requests from the wireless communication devices at the gateway module and transferring the checkout requests to a wallet module that manages user authentication (Nguyen, fig. 28:2830, 2850-2882);

when a user at a wireless communications device has logged-in to the wallet module, transmitting payment options from the wallet module to the wireless communications device in

response to a checkout request from the wireless communications device (Nguyen, fig. 27:2708,2704);

when a user at a wireless communications device has not logged-in to the wallet module, transmitting a log-in prompt from the wallet module to the wireless communications device in response to a checkout request from the wireless communications device (Nguyen, fig. 31).

Regarding claim 7, it is rejected, at least, for the same reasons as claims 2 and 3.

Regarding claim 8, the combination discloses:

in response to a payment request from a wireless communications device, transmitting the payment request from the gateway module to the merchant application (Nguyen, fig. 3, 28);

disassociating the wireless session identifier from the corresponding merchant session identifier (66:25-30),

generating a new wireless session identifier for the wireless communications device when another initial request is received from the wireless communications device (see the above claims for repeating the disclosed process).

Regarding claim 9, the combination discloses:

clearing inactive entries from the wallet session identifier table (Nguyen, 66:25-30, 53-60).

Regarding claim 10, it is rejected, at least, for the same reasons as claims 1 and 5.

Regarding claims 11 – 13, they are system implementing the method of claims 1 – 3, and they are rejected, at least, for the same reasons.

(10) Response to Argument

Appellant's arguments filed 2/28/2008 have been fully considered but they are not persuasive. Appellant asserts or argues primarily that:

(i) *That is neither Aziz nor Kocher teaches or suggests the second session identifier, which the application provided to the gateway, is transmitted back to the application from the gateway for the subsequent communications.* (Brief, pg. 15, par. 1)

In response, the examiner respectfully notes that the during the server-client ssl handshake (e.g. for the initiation of an SSL session), the server sends a session identifier within a 'Server hello message' so as to identify a communication session (Kocher, pg. 23, sect. 7.6.1.3 – pg. 24, "session_id"). When the gateway resumes this communication session, it sends the same session identifier, as was sent by the server within the 'Server hello message', within a 'Client hello message' (Kocher, pg. 19, par. 1, 2). Thus, the examiner points out that the prior art does disclose transmitting from the gateway module the second session identifier back to the application program.

(ii) *Thus, the client does not send a hello message for each subsequent communication between the client and the server. Hence, once the two different secure connections are established between the client and the relay and between the relay and the server respectively, hello messages are not exchanged for each subsequent communication from the client. Thus, Aziz fails to teach in response to each subsequent communication from each mobile device to the application program, while the*

connection is established, transmitting from the gateway module to the application program the second session identifier. (Brief, pg. 15, par. 3)

In response, the examiner respectfully notes, contrary to the assertions of the appellant, the prior art teaches that subsequent communications over an established SSL link require the initiation of a session resumption procedure (Aziz, 2:57-61). A session resumption procedure between the gateway and application program involves the sending of hello messages comprising the session identifiers (Kocher, pg. 19, par. 1, 2).

(iii) *Furthermore, Aziz discloses two different secure connections are established between the client and the relay and between the relay and the server, respectively. Thus, hello messages or session identifiers for the first secure connection and the second secure connection are not associated in Aziz. Hence, Aziz fails to teach "associating the first session identifiers with corresponding second session identifiers from the application program at the gateway module," as cited in claim 1.* (Brief, pg. 16, par. 1)

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is respectfully noted that the features upon which appellant bases his argument upon (*session identifiers for the first secure connection and the second secure connection are not associated* - i.e. the association of session identifiers for a first secure connection and a second secure connection) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(iv) *Independent claims 5 and 10 recite features similar to claim 1 described above which are not taught or suggested by Aziz in view of Davis.* (Brief, pg. 18, par. 2)

In response, the examiner respectfully notes that the appellant's argument is based upon the arguments above, and is found to be unpersuasive for the same reasons.

(v) *However, there is no apparent element in this portion of Sparks or Aziz that corresponds to the gateway module at which checkout requests are received or the claimed wallet module to which the checkout requests are sent. Furthermore, the wallet module and its corresponding claimed features described above are not taught or suggested.* (Brief, pg. 18, par. 3)

In response, the examiner respectfully notes that the prior art combination enables for client devices to engage in electronic commerce, including the issuing of checkout requests to a server (Sparks, col. 2, lines 36-49). Since all communication from a client device to a server is received by the gateway module (Aziz, fig. 2, 6), the examiner notes that any checkout requests from a client are received at the gateway module. Additionally, the prior art combination enables a “wallet module”, that receives checkout requests and authenticates a user via login id and password (Sparks, col. 2, lines 36-49; 5:41-43; 16:57-67).

Furthermore, in response to the assertion *the wallet module and its corresponding claimed features described above are not taught or suggested,* the examiner respectfully notes that Appellant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

(vi) *However, there is no apparent suggestion in either of Aziz or Sparks that any disassociation takes palace in response to a payment request as claimed.* (Brief, pg. 19, par. 1).

In response, the examiner respectfully notes the appellant fails to claim any specific manner or means of association/disassociation. The prior art teaches that unless session resumption procedures have been initiated by the client or the server, the session identifiers of the client are not re-associated with the corresponding session identifiers of the server, therefore, for all intents and purposes, they are disassociated. (Aziz, col. 2, lines 57-67; col. 6, lines 45-55).

(vii) *Thus, the TID field 2005, which is allegedly the claimed second session identifiers, is generated by the POS and not the bank, which is allegedly the claimed application. Hence, Nguyen fails to teach or suggest second session identifiers from an application, as claimed in claim 1.* (Brief, pg. 20)

In response, the examiner notes that the appellant's argument appears to be based upon where the second session identifier of the prior art *is generated*. The examiner respectfully notes that "from an application" is not equivalent to 'generated by an application'. In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., where the second session identifier is generated) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The examiner notes that the prior art reveals a system (fig. 20C, similarly fig. 22) disclosing a plurality of clients (fig. 20C:2000) engaged in a corresponding plurality of customer-institution

sessions (fig. 20C:2003) with an application (fig. 20C:2004) via a gateway (fig. 20C:2007). Second session identifiers from the application (fig. 20:2005) are associated with the first session identifiers (fig. 20C:2010, see also 64:36-38) generated by the gateway to uniquely represent a corresponding transaction request received from a client. Thus, the examiner notes that the prior art discloses second session identifiers from an application.

(viii) *Claim 1 also recites, "wherein respective connections are established between the mobile communications device and the application program." Nguyen fails to teach or suggest establishing connection between mobile communications devices and the application program. Instead, in Nguyen, the clients 2000 communicate with the VPOS terminal to perform a transaction such as a payment. The VPOS communicates with the bank 2004 on a separate connection 2003 shown in figure 20C. The clients 2000 are not attempting to communicate with the bank 2004, and there is no connection established between the clients 2000 and the bank 2004.* (Brief, pg. 21, par. 1)

In response, the examiner respectfully notes that between a client and the bank ("application program"), there is located a connection (fig. 20C:2003). As the prior art teaches that the connection exists between the client and the application program, the examiner notes that the prior art teaches an established connection *between mobile communications devices and the application program.*

Furthermore, the examiner notes that the prior art teaches that the customer or client is issuing payment or account requests so that the bank will pay the merchant on behalf of the customer. These requests by the customer are delivered to the bank. Thus, the examiner notes that the client or customer is in communication with the bank or application program (Nguyen, Abstract; 65:38-47).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffery Williams/

Examiner, Art Unit 2137

Conferees:

/Christopher A. Revak/

Primary Examiner, Art Unit 2131

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135